What is claimed is:

1. A digital content protection system that enables a digital content to be used and includes a recording medium apparatus having a storage area for holding digital content information and an access apparatus that reads information from and writes information into the storage area,

the digital content protection system operating according to the following phases:

an authentication phase where the recording medium apparatus secretly transmits an inherent key to the access apparatus, and the recording medium apparatus and the access apparatus perform mutual authentication using the inherent key, the inherent key being information that is unique to the recording medium apparatus; and

a content transfer phase, performed only when the recording medium apparatus and the access apparatus have successfully authenticated each other, where the access apparatus either (a) encrypts a digital content using the secretly transmitted inherent key and sends the encrypted digital content to the recording medium apparatus or (b) receives an encrypted digital content from the recording medium apparatus and decrypts the encrypted digital content using the secretly transmitted inherent key.

2. The digital content protection system of Claim 1,

wherein the recording medium apparatus includes a first calculation means, and

the access apparatus includes a first authentication information generating means and a first authentication means,

wherein while the access apparatus judges whether the recording medium apparatus is legitimate in the authentication phase,

the first authentication information generating means generates first authentication information and outputs the first authentication information to the recording medium apparatus,

the first calculation means receives the first authentication information, generates first calculated authentication information by performing a first calculation on the received first authentication information using the inherent key, and outputs the first calculated authentication information to the access apparatus, and

the first authentication means judges whether the recording medium apparatus is legitimate from the first authentication information and the first calculated authentication information using the secretly transmitted inherent key.

3. The digital content protection system of Claim 2,

wherein the access apparatus includes a second calculation means, and

the recording medium apparatus includes a second authentication information generating means and a second authentication means,

wherein while the recording medium apparatus judges whether the access apparatus is legitimate in the authentication phase,

the second authentication information generating means generates second authentication information and outputs the second authentication information to the access medium apparatus,

the second calculation means receives the second authentication information, generates second calculated authentication information by performing a second calculation on the received second authentication information using the secretly transmitted inherent key, and outputs the second calculated authentication information to the recording medium apparatus, and

the second authentication means judges whether the access apparatus is legitimate from the second authentication information and the second calculated authentication information using the inherent key.

4. The digital content protection system of Claim 3,

wherein the recording medium apparatus further includes a first encryption means and an inherent key storing means for prestoring the inherent key, and

the access apparatus further includes a first decryption means,

wherein while the recording medium apparatus secretly transmits the inherent key to the access apparatus in the authentication phase,

the first encryption means generates an encrypted inherent key by applying a first encryption algorithm to the inherent key and outputs the encrypted inherent key to the access apparatus, and

the first decryption means receives the encrypted inherent key and generates a decrypted inherent key by applying a first decryption algorithm to the encrypted inherent key, the first decryption algorithm being used to decrypt cipher text generated with the first encryption algorithm.

5. The digital content protection system of Claim 4,

wherein the recording medium apparatus further includes a first key storing means for prestoring a first key, and

the access apparatus further includes a second key storing means for prestoring a second key that corresponds to the first key,

wherein the first encryption means encrypts the inherent key using the first key, and

the first decryption means decrypts the encrypted inherent key using the second key.

6. The digital content protection system of Claim 5,

wherein the first key and the second key are the same master key, and

the first decryption means decrypts the encrypted inherent key using the second key that is the same as the

first key.

7. The digital content protection system of Claim 5,

wherein the first key is a public key that is calculated from the second key according to a public key determination algorithm of a public key cryptosystem,

the first encryption algorithm is an encryption algorithm of the public key cryptosystem, and

the first decryption algorithm is a decryption algorithm of the public key cryptosystem,

wherein the first encryption means encrypts the inherent key according to the encryption algorithm of the public key cryptosystem using the first key that is the public key, and

the first decryption means decrypts the encrypted inherent key according to the decryption algorithm of the public key cryptosystem using the second key.

8. The digital content protection system of Claim 5,

wherein the second key is a public key that is calculated from the first key according to a public key determination algorithm of a recovery signature processing method,

the first encryption algorithm is a signature processing algorithm of the recovery signature processing method,

the first encryption means generates the encrypted inherent key that is a signature text by applying the first

encryption algorithm to the inherent key using the first key,

the first decryption algorithm is a verification processing algorithm of the recovery signature processing method, and

the first decryption means generates the decrypted inherent key by applying the first decryption algorithm to the encrypted inherent key that is the signature text using the second key.

9. The digital content protection system of Claim 4,

wherein the recording medium apparatus further includes:

a first master key storing means for prestoring a first master key group that includes a plurality of master keys; and

a first selection means for selecting a master key out of the first master key group as a first key, and

the access apparatus further includes:

a second master key storing means for prestoring a second master key group that includes a plurality of master keys, the first master key group and the second master key group include the same plurality of master keys; and

a second selection means for selecting a master key out of the second master key group as a second key, the second key being the same as the first key,

wherein the first encryption means encrypts the inherent key using the master key selected as the first key,

and

the first decryption means decrypts the encrypted inherent key using the master key selected as the second key.

10. The digital content protection system of Claim 4,

wherein the first encryption means prestores a first subgroup key, generates a transformed key by performing a first conversion on the inherent key using the first subgroup key, and generates the encrypted inherent key by applying the first encryption algorithm to the transformed key, and

the first decryption means prestores a second subgroup key that is the same as the first subgroup key, generates a decrypted transformed key by applying the first decryption algorithm to the encrypted inherent key, and generates the decrypted inherent key by performing an inversion operation of the first conversion operation on the decrypted transformed key using the second subgroup key.

11. The digital content protection system of Claim 4,

wherein the first encryption means prestores a first subgroup key, generates a cipher text by applying the first encryption algorithm to the inherent key, and generates the encrypted inherent key by performing a first conversion operation on the cipher text using the first subgroup key, and

the first decryption means prestores a second subgroup key that is the same as the first subgroup key,

generates a decryption text by performing an inverse operation of the first conversion operation on the encrypted inherent key using the second subgroup key, and generates the decrypted inherent key by applying the first decryption algorithm to the decryption text.

12. The digital content protection system of Claim 4,

wherein the recording medium apparatus further includes a first key storing means for prestoring a first key that is a master key, and

the access apparatus further includes a second key storing means for prestoring a second key that is the same master key as the first key,

wherein the first encryption means prestores a first subgroup key, generates an encrypted first key by performing a first conversion operation on the first key using the first subgroup key, and generates the encrypted inherent key by applying the first encryption algorithm to the inherent key using the encrypted first key, and

the first decryption means prestores a second subgroup key that is the same as the first subgroup key, generates an encrypted second key by performing a second conversion operation, which is the same as the first conversion operation, on the second key using the second subgroup key, and generates the decrypted inherent key by applying the first decryption algorithm to the encrypted inherent key using the encrypted second key.

13. The digital content protection system of Claim 3, wherein the first authentication means includes:

a third calculation means for generating third calculated authentication information by performing a third calculation that is the same as the first calculation on the first authentication information using the secretly transmitted inherent key; and

a first comparison means for judging whether the first calculated authentication information matches the third calculated authentication information and, if so, determining that the recording medium apparatus is legitimate.

14. The digital content protection system of Claim 13, wherein the second authentication means includes:

a fourth calculation means for generating fourth calculated authentication information by performing a fourth calculation that is the same as the second calculation on the second authentication information using the inherent key; and

a second comparison means for comparing the second calculated authentication information with the fourth calculated authentication information and judging, when the second calculated authentication information matches the fourth calculated authentication information, that the access apparatus is legitimate.

15. The digital content protection system of Claim 14, wherein the first calculation means prestores a first

subgroup key, generates a transformed inherent key by performing a first conversion operation on the inherent key using the subgroup key, and generates the first calculated authentication information by performing the first calculation on the first authentication information using the transformed inherent key, and

the third calculation means prestores a second subgroup key that is the same as the first subgroup key, generates a decrypted transformed inherent key by performing an inversion operation of the first conversion operation on the secretly transmitted inherent key using the subgroup key, and generates the third calculated authentication information by performing a calculation that is the same as the first calculation on the first authentication information using the decrypted transformed inherent key.

16. The digital content protection system of Claim 14,

wherein the first authentication information generating means generates a random number as the first authentication information, and

the second authentication information generating means generates a random number as the second authentication information.

17. The digital content protection system of Claim 3,

wherein the first calculation is a first encryption algorithm,

the first calculation means generates the first

calculated authentication information by applying the first encryption algorithm to the first authentication information using the inherent key, and

the first authentication means generates first decrypted authentication information by applying a first decryption algorithm to the first calculated authentication information using the secretly transmitted inherent key, compares the first authentication information with the first decrypted authentication information, and judges, when the first authentication information matches the first decrypted authentication information, that the recording medium apparatus is legitimate,

wherein the first decryption algorithm is used to decrypt a cipher text generated using the first encryption algorithm.

18. The digital content protection system of Claim 17,

wherein the second calculation is a second encryption algorithm,

the second calculation means generates the second calculated authentication information by applying the second encryption algorithm to the second authentication information using the secretly transmitted inherent key, and

the second authentication means generates second decrypted authentication information by applying a second decryption algorithm to the second calculated authentication information using the inherent key, compares the second authentication information with the second decrypted

authentication information, and judges, when the second authentication information matches the second decrypted authentication information, that the access apparatus is legitimate,

wherein the second decryption algorithm is used to decrypt a cipher text generated using the second encryption algorithm.

19. The digital content protection system of Claim 18,

wherein the first calculation means prestores a first subgroup key, generates a transformed inherent key by performing a first conversion on the inherent key using the first subgroup key, and generates the first calculated authentication information by applying the first encryption algorithm to the first authentication information using the transformed inherent key, and

the first authentication means prestores a second subgroup key that is the same as the first subgroup key, generates a decrypted transformed inherent key by performing an inversion operation of the first conversion on the secretly transmitted inherent key using the second subgroup key, and generates the first decrypted authentication information by applying the first decryption algorithm to the first calculated authentication information using the decrypted transformed inherent key.

20. The digital content protection system of Claim 18,

wherein the first authentication information

generating means generates a random number as the first authentication information, and

the second authentication information generating means generates a random number as the second authentication information.

21. The digital content protection system of Claim 3,

wherein the storage area holds digital content information that is generated by applying an encryption algorithm to a digital content using the inherent key,

the recording medium apparatus further includes an output means for reading, when the recording medium apparatus and the access apparatus have successfully authenticated each other, the digital content information from the storage area and outputting the read digital content information to the access apparatus, and

the access apparatus that reads information from the storage area further includes:

a content decryption means for receiving the digital content information from the recording medium apparatus and generating a decrypted digital content by applying a decryption algorithm to the digital content information using the secretly transmitted inherent key, the decryption algorithm being used to decrypt a cipher text generated using the encryption algorithm; and

a reproduction means for reproducing the decrypted digital content.

22. The digital content protection system of Claim 3,

wherein the access apparatus that writes information into the storage area further includes:

a content obtaining means for obtaining a digital content from the outside; and

a content encryption means for generating digital content information by applying an encryption algorithm to the obtained digital content using the secretly transmitted inherent key, and outputting the digital content information to the recording medium apparatus,

wherein the storage area holds the outputted digital content information.

23. The digital content protection system of Claim 1,

wherein when the recording medium apparatus and the access apparatus have successfully authenticated each other,

in the content transfer phase, the access apparatus either

(c) generates at least one data block by dividing a digital content, generates a data block key for each data block, generates at least one encrypted data block by encrypting each data block using the secretly transmitted inherent key and a data block key that corresponds to the data block, and transfers each encrypted data block to the recording medium, or

(d) receives at least one encrypted data block of an encrypted digital content from the recording medium

apparatus, generates a data block key for each data block, and generates at least one data block by decrypting each encrypted data block using the secretly transmitted inherent key and a data block key that corresponds to the encrypted data block,

wherein each data block has one of a logical length and a physical length, and

each encrypted data block has one of a logical length and a physical length.

24. The digital content protection system of Claim 1,

wherein when the recording medium apparatus and the access apparatus have successfully authenticated each other,

in the content transfer phase, the access apparatus either

(e) generates a file key for a file of a digital content, generates an encrypted file by encrypting the file using the secretly transmitted inherent key and the file key, and transfers the encrypted file and information concerning the file key to the recording medium, or

(f) receives, from the recording medium apparatus, an encrypted file of an encrypted digital content and information concerning a file key that corresponds to the encrypted file, generates a decrypted file by decrypting the encrypted file using the secretly transmitted inherent key and the information concerning the file key, and reproduces the decrypted file.

25. The digital content protection system of Claim 24, wherein when the recording medium apparatus and the access apparatus have successfully authenticated each other,

in the content transfer phase, the access apparatus either

(g) generates a file key for a file of a digital content, generates an encrypted file by encrypting the file using the file key, generates an encrypted file key by encrypting the file key using the secretly transmitted inherent key, and transfers the encrypted file and the encrypted file key to the recording medium, or

(h) receives, from the recording medium apparatus, an encrypted file and an encrypted file key that corresponds to the encrypted file, generates a file key by decrypting the encrypted file key using the secretly transmitted inherent key, generates a decrypted file by decrypting the encrypted file using the file key, and reproduces the decrypted file.

26. The digital content protection system of Claim 24, wherein the recording medium apparatus generates a seed from a current time and outputs the seed to the access apparatus, the seed being an initial value of a random number,

the access apparatus receives the generated seed from the recording medium apparatus, generates the random number from the seed, and sets the random number as a file key.

27. The digital content protection system of Claim 24,

wherein while the access apparatus judges whether the recording medium apparatus is legitimate in the authentication phase,

the access apparatus sends the first authentication information to the recording medium apparatus,

the recording medium apparatus generates a seed from a current time, generates a combination result by combining the seed with the first authentication information, generates an encrypted combination result by encrypting the combination result using the inherent key, and sends the encrypted combination result to the access apparatus, the seed being an initial value of a random number, and

the access apparatus generates a decrypted seed and first decrypted authentication information by decrypting the encrypted combination result using the secretly transmitted inherent key, judges whether the first authentication information matches the first decrypted authentication information, and, if so, determines that the recording medium apparatus is legitimate, and

in the content transfer phase, the access apparatus generates the random number from the decrypted seed and sets the random number as a file key.

28. The digital content protection system of Claim 1,

wherein when the recording medium apparatus and the access apparatus have successfully authenticated each

other,

in the content transfer phase, the access apparatus either

(i) receives a user key from an operator, generates a transformed key from the user key and the secretly transmitted inherent key, generates an encrypted digital content by encrypting a digital content using the transformed key, and transfers the encrypted digital content to the recording medium, or

(j) receives an encrypted digital content from the recording medium apparatus, generates a transformed key from a user key inputted from an operator and the secretly transmitted inherent key, and generates a decrypted digital content by decrypting the encrypted digital content using the transformed key.

29. The digital content protection system of Claim 1,

wherein when the recording medium apparatus and the access apparatus have successfully authenticated each other,

in the content transfer phase, the access apparatus either

(k) receives a user key from an operator, generates a file key for a file of a digital content, generates a transformed key from the user key and the file key, generates an encrypted file by encrypting the file using the transformed key, and transfers the encrypted file and the transformed key to the recording medium, or

(1) receives, from the recording medium apparatus, an encrypted file and a transformed key that corresponds to the encrypted file, receives a user key from an operator, generates a file key from the user key and the transformed key, generates a decrypted file by decrypting the encrypted file using the file key, and reproduces the decrypted file.

30. The digital content protection system of Claim 1,

wherein while the recording medium apparatus judges whether the access apparatus is legitimate in the authentication phase,

the recording medium apparatus sends second authentication information to the access apparatus,

the access apparatus generates encrypted second authentication information by encrypting the second authentication information using a master key and sends the encrypted second authentication information to the recording medium apparatus, and

the recording medium apparatus generates decrypted second authentication information by decrypting the encrypted second authentication information using a master key, judges whether the second authentication information matches the decrypted second authentication information, and, if so, determines that the access apparatus is legitimate.

31. The digital content protection system of Claim 1 further includes an encrypted inherent key generation apparatus,

wherein the digital content protection system further operates according to an encrypted inherent key setting phase where the encrypted inherent key generation apparatus generates an encrypted inherent key by encrypting the inherent key sent from the recording medium apparatus and sends the encrypted inherent key to the recording medium apparatus, and the recording medium apparatus holds the encrypted inherent key sent from the encrypted inherent key generation apparatus,

wherein in the authentication phase, the recording medium apparatus sends the encrypted inherent key to the access apparatus, and the access apparatus generates a decrypted inherent key by decrypting the encrypted inherent key secretly sent from the recording medium apparatus and judges whether the recording medium apparatus is legitimate using the decrypted inherent key.

32. A recording medium apparatus that has a storage area for holding digital content information and is used in a digital content protection system,

wherein the digital content protection system enables a digital content to be used and further includes an access apparatus that reads information from and writes information into the storage area, and

the digital content protection system operates according to the following phases:

an authentication phase where the recording medium apparatus secretly transmits an inherent key to the access

apparatus, and the recording medium apparatus and the access apparatus perform mutual authentication using the inherent key, the inherent key being information that is unique to the recording medium apparatus; and

a content transfer phase, performed only when the recording medium apparatus and the access apparatus have successfully authenticated each other, where the access apparatus either (a) encrypts a digital content using the secretly transmitted inherent key and sends the encrypted digital content to the recording medium apparatus or (b) receives an encrypted digital content from the recording medium apparatus and decrypts the encrypted digital content using the secretly transmitted inherent key.

33. The recording medium apparatus of Claim 32,

wherein the recording medium apparatus includes a first calculation means, and

the access apparatus includes a first authentication information generating means and a first authentication means,

wherein while the access apparatus judges whether the recording medium apparatus is legitimate in the authentication phase,

the first authentication information generating means generates first authentication information and outputs the first authentication information to the recording medium apparatus,

the first calculation means receives the first

authentication information, generates first calculated authentication information by performing a first calculation on the received first authentication information using the inherent key, and outputs the first calculated authentication information to the access apparatus, and

the first authentication means judges whether the recording medium apparatus is legitimate from the first authentication information and the first calculated authentication information using the secretly transmitted inherent key.

34. The recording medium apparatus of Claim 33,

wherein the access apparatus includes a second calculation means, and

the recording medium apparatus includes a second authentication information generating means and a second authentication means,

wherein while the recording medium apparatus judges whether the access apparatus is legitimate in the authentication phase,

the second authentication information generating means generates second authentication information and outputs the second authentication information to the access medium apparatus,

the second calculation means receives the second authentication information, generates second calculated authentication information by performing a second calculation on the received second authentication information using the

secretly transmitted inherent key, and outputs the second calculated authentication information to the recording medium apparatus, and

the second authentication means judges whether the access apparatus is legitimate from the second authentication information and the second calculated authentication information using the inherent key.

35. An access apparatus that reads information from and writes information into a storage area of a recording medium apparatus and is included in a digital content protection system,

wherein the storage area holds digital content information,

the digital content protection system enables a digital content to be used and includes the recording medium apparatus and the access apparatus,

wherein the digital content protection system operates according to the following phases:

an authentication phase where the recording medium apparatus secretly transmits an inherent key to the access apparatus, and the recording medium apparatus and the access apparatus perform mutual authentication using the inherent key, the inherent key being information that is unique to the recording medium apparatus; and

a content transfer phase, performed only when the recording medium apparatus and the access apparatus have successfully authenticated each other, where the access

apparatus either (a) encrypts a digital content using the secretly transmitted inherent key and sends the encrypted digital content to the recording medium apparatus or (b) receives an encrypted digital content from the recording medium apparatus and decrypts the encrypted digital content using the secretly transmitted inherent key.

36. The access apparatus of Claim 35,

wherein the recording medium apparatus includes a first calculation means, and

the access apparatus includes a first authentication information generating means and a first authentication means,

wherein while the access apparatus judges whether the recording medium apparatus is legitimate in the authentication phase,

the first authentication information generating means generates first authentication information and outputs the first authentication information to the recording medium apparatus,

the first calculation means receives the first authentication information, generates first calculated authentication information by performing a first calculation on the received first authentication information using the inherent key, and outputs the first calculated authentication information to the access apparatus, and

the first authentication means judges whether the recording medium apparatus is legitimate from the first

authentication information and the first calculated authentication information using the secretly transmitted inherent key.

37. The access apparatus of Claim 36,

wherein the access apparatus includes a second calculation means, and

the recording medium apparatus includes a second authentication information generating means and a second authentication means,

wherein while the recording medium apparatus judges whether the access apparatus is legitimate in the authentication phase,

the second authentication information generating means generates second authentication information and outputs the second authentication information to the access medium apparatus,

the second calculation means receives the second authentication information, generates second calculated authentication information by performing a second calculation on the received second authentication information using the secretly transmitted inherent key, and outputs the second calculated authentication information to the recording medium apparatus, and

the second authentication means judges whether the access apparatus is legitimate from the second authentication information and the second calculated authentication information using the inherent key.

38. An encrypted inherent key generating apparatus that is used in a digital content protection system,

wherein the digital content protection system that enables a digital content to be used and includes a recording medium apparatus having a storage area for holding digital content information and an access apparatus that reads information from and writes information into the storage area,

the digital content protection system operating according to the following phases:

an encrypted inherent key setting phase where the encrypted inherent key generation apparatus generates an encrypted inherent key by encrypting the inherent key sent from the recording medium apparatus and sends the encrypted inherent key to the recording medium apparatus, and the recording medium apparatus holds the encrypted inherent key sent from the encrypted inherent key generation apparatus, wherein the inherent key is information that is unique to the recording medium apparatus;

an authentication phase where the recording medium apparatus transmits the encrypted inherent key to the access apparatus, the access apparatus generates an decrypted inherent key by decrypting the encrypted inherent key transmitted from the recording medium apparatus, the recording medium apparatus judges whether the access apparatus is an authorized apparatus using the inherent key, and the access apparatus judges whether the recording medium

apparatus is an authorized apparatus using the decrypted inherent key; and

a content transfer phase, performed only when the recording medium apparatus and the access apparatus have successfully authenticated each other, where the access apparatus either (a) encrypts a digital content using the decrypted inherent key and sends the encrypted digital content to the recording medium apparatus or (b) receives an encrypted digital content from the recording medium apparatus and decrypts the encrypted digital content using the decrypted inherent key.

39. A digital content protection method used in a digital content protection system that enables a digital content to be used and includes a recording medium apparatus having a storage area for holding digital content information and an access apparatus that reads information from and writes information into the storage area,

the digital content protection method comprising:

an authentication step where the recording medium apparatus secretly transmits an inherent key to the access apparatus, and the recording medium apparatus and the access apparatus perform mutual authentication using the inherent key, the inherent key being information that is unique to the recording medium apparatus; and

a content transfer step, performed only when the recording medium apparatus and the access apparatus have successfully authenticated each other, where the access

apparatus either (a) encrypts a digital content using the secretly transmitted inherent key and sends the encrypted digital content to the recording medium apparatus or (b) receives an encrypted digital content from the recording medium apparatus and decrypts the encrypted digital content using the secretly transmitted inherent key.

40. A digital content protection program that is recorded on a computer-readable recording medium and is executed in a digital content protection system,

wherein the digital content protection system enables a digital content to be used and includes a recording medium apparatus having a storage area for holding digital content information and an access apparatus that reads information from and writes information into the storage area,

the digital content protection program comprising:

an authentication step where the recording medium apparatus secretly transmits an inherent key to the access apparatus, and the recording medium apparatus and the access apparatus perform mutual authentication using the inherent key, the inherent key being information that is unique to the recording medium apparatus; and

a content transfer step, performed only when the recording medium apparatus and the access apparatus have successfully authenticated each other, where the access apparatus either (a) encrypts a digital content using the secretly transmitted inherent key and sends the encrypted digital content to the recording medium apparatus or (b)

receives an encrypted digital content from the recording medium apparatus and decrypts the encrypted digital content using the secretly transmitted inherent key.

41. A computer digital signal that is sent via a communication channel and includes a digital content protection program used in a digital content protection system,

wherein the digital content protection system enables a digital content to be used and includes a recording medium apparatus having a storage area for holding digital content information and an access apparatus that reads information from and writes information into the storage area,

the digital content protection program comprising:

an authentication step where the recording medium apparatus secretly transmits an inherent key to the access apparatus, and the recording medium apparatus and the access apparatus perform mutual authentication using the inherent key, the inherent key being information that is unique to the recording medium apparatus; and

a content transfer step, performed only when the recording medium apparatus and the access apparatus have successfully authenticated each other, where the access apparatus either (a) encrypts a digital content using the secretly transmitted inherent key and sends the encrypted digital content to the recording medium apparatus or (b) receives an encrypted digital content from the recording medium apparatus and decrypts the encrypted digital content

using the secretly transmitted inherent key.